



*Information Systems
Audit and Control
Association*

News

Nr. 63, April 2003

Letter

Thema

Registerharmonisierung

Switzerland Chapter
Germany Chapter
Austria Chapter

© 22.4.2003

Impressum

Herausgeber:

ISACA Switzerland Chapter

c/o Monika Josi

PricewaterhouseCoopers AG

Nordstrasse 15

8035 Zürich

Redaktion:

Max F. Bretscher

KPMG Fides Peat

Badenerstrasse 172

8026 Zürich

Satz und Gestaltung:

WissensTransfer

Francesca Lüscher Baglioni,

8235 Lohn, SH

Jeder Nachdruck, auch auszugsweise, sowie Vervielfältigungen oder sonstige Verwertung von Texten oder Abbildungen aus dem Newsletter nur mit schriftlicher Genehmigung des Herausgebers unter voller Quellenangabe.

Inserate:

1 Seite CHF 400.–

1/2 Seite CHF 240.–

1/4 Seite CHF 160.–

Erscheint 5 Mal jährlich

Auflage: 1000 Exemplare

Nächste Ausgabe (Thema: Katastrophenfallplan): Juni 2003, Redaktionsschluss: 10. Juni 2003

Inhaltsverzeichnis

Editorial	4
Registerharmonisierung – Harmonisierung amtlicher Personenregister	6
Registerharmonisierung – Identifier Fritz Müller pour mieux le protéger !	8
Registerharmonisierung – Die registrierte Gesellschaft	9
Datenschutz – Datenschutz im Data Warehouse	10
Datenschutz – Some Provocative Thoughts on Data Protection	14
Konfliktmediation – Ein neues Berufsbild?	16
The ISACA Crossword Puzzle	20
News aus den Interessengruppen	21
Express Line	23
DACH-News	24
Veranstaltungen	27
Germany Chapter	29
Austria Chapter	30
Switzerland Chapter	31

Editorial

Bürgerin 23802

Angesichts der verschiedenen Kredit- und Mitgliedskarten frage ich mich manchmal, in wie vielen Systemen ich als Nummer existiere. Nehmen wir zum Beispiel das Kundenbindungsprogramm eines grossen Lebensmittelverteilers. Der Anreiz für mich sind Bonuspunkte, mit welchen ich vom Toaster bis zu Flugreisen so ziemlich alles erstehen kann. Dort bin ich als Kundin 12345 bekannt, meine Einkäufe sind genauestens erfasst und auswertbar. Auswertungen, die so hoffe ich, vielleicht in ein auf mich zugeschnittenes Dienstleistungsangebot resultieren: Vermehrt frisches Brot auch noch um 19.30 Uhr abends oder ein grösseres Angebot von Bioprodukten. Ein positiver Effekt für mich. Doch was passieren sonst noch für Auswertungen? Die Analyse meiner Alkoholeinkäufe, meines Eintausches der Prämie in Flugmeilen und mit wem ich diesen Bonus eingelöst habe? Besteht hier die Gefahr von Missbrauch? Wie bin ich hier geschützt?

Ähnlich verhält es sich mit dem an der letzten ISACA Generalversammlung vorgestellten Projekt zur Harmonisierung amtlicher Personenregister auf eidgenössischer Ebene. Ziel ist ein einheitlicher Personenidentifikator zur Erleichterung von statistischen Auswertungen und eine höhere Datenqualität. Als Bürgerin 23802 wird mein Weg- und Zuzug aus Gemeinden und Kantonen nachvollziehbar, sie erleichtert meine

Identifikation im elektronischen Verkehr im e-government und hilft, verwaltungsinterne Abläufe zu optimieren. Mögliche positive Erscheinungen für mich: Eine bessere Planungsgrundlage für Bund und Kantone für den Schienen- und Strassenbau (und somit hoffentlich weniger Stau und genügend Sitzplätze in Pendlerzügen), die Möglichkeit, an e-voting teilzunehmen sowie eine schnellere und kundenfreundlichere Interaktion mit Bund, Kantonen und Gemeinden. Doch was ist sonst noch möglich mit dieser Information? Kann ausgewertet werden, mit wem ich zusammen von wann bis wann in welcher Gemeinde gelebt habe? Und wie gross die gemeinsame Wohnung war?

Auch hier stellt sich die Frage, wie Missbrauch dieser Daten verhindert werden kann. Ich bin gerne bereit, als Bürgerin 23802 erfasst zu werden, möchte aber die Gewissheit haben, dass Kontrollen implementiert werden, die einen Missbrauch verhindern. Und dass diese Kontrolle nicht nur auf Papier bestehen, sondern dass diese eingehalten werden und diese Einhaltung auch regelmässig überprüft wird.

Das ISACA Chapter Switzerland wird in einer Stellungnahme zu der bis zum 30. April 2003 laufenden Vernehmlassung des Bundes ihren Standpunkt zu diesem Projekt darlegen. Ein Zeichen, dass unser Chapter nicht nur auf dem Papier existiert, sondern sich aktiv am politischen Geschehen beteiligt.

Citoyenne 23802

Lorsque je jette un coup d'œil à mes différentes cartes plastifiées, je me demande parfois combien de systèmes m'ont déjà attribué un numéro. Prenons l'exemple du système mis en place par une grande chaîne de distribution alimentaire pour fidéliser sa clientèle. Pour obtenir des bons d'achat à faire valoir sur l'achat d'un toaster ou sur mon prochain vol, je suis disposée à être numérotée « cliente 12345 » et à laisser le vendeur suivre mes achats à la trace. Je peux également profiter de cette curiosité : elle pourra peut-être amener le vendeur à analyser systématiquement mon comportement et mes besoins et à me mettre à disposition du pain frais à 19 heures 30 ou à étendre son offre de produits bio. Est-ce tout ? Ou dois-je craindre une analyse de ma consommation d'alcool, des destinations de mes vols ou de la personne qui volera en ma compagnie ? Quels sont les risques ? Comment suis-je protégée ?

Même problématique avec le thème abordé lors de l'Assemblée générale de l'ISACA : le projet d'harmonisation des registres de personnes et l'éventuelle création d'un numéro d'identification personnel. Ce projet devrait permettre de simplifier les travaux statistiques et d'améliorer la qualité des données. Mon parcours de « citoyenne 23802 » sera suivi au fil de mes déménagements de commune à commune, voire de canton à canton. Ce numéro « 23802 » facilitera mes contacts avec les guichets

virtuels des différentes administrations et permettra à celles-ci d'être plus efficaces. Je profiterai peut-être également d'une amélioration de la planification routière et ferroviaire (moins de bouchons sur les routes et assez de places assises dans les trains pendulaires), je pourrai participer aux votations électroniques et disposer d'une administration efficace et souriante qui aura harmonisé ses processus aux échelons communal, cantonal et fédéral. Mais de nouveau : ces informations ne pourraient-elles pas être détournées de leur but ? Sera-t-il possible de reconstituer ma vie sentimentale : avec qui ai-je habité, durant combien de temps et quelle était la taille de notre appartement ?

On en revient toujours à la même question : comment empêcher efficacement les abus ? Je suis prête à être la citoyenne 23802, mais je veux être sûre que des contrôles ont été mis en place pour empêcher un usage abusif de mes données. Et que ces contrôles ne figurent pas que sur le papier mais que leur efficacité est régulièrement auditée !

Le chapitre suisse de l'ISACA prendra position d'ici fin avril 2003 sur ce projet. Un signe que notre association ne se contente pas d'exister sur le papier mais prend une part active à la vie politique de ce pays !

Monika Josi

1

An auditor worked in the land of Northumber
She was very diligent and did never slumber
The opposite – she was very awake
And all the problems did brake;
But unfortunately she was only a number.

8

Vor viel hundert Jahr lebte einst im Land der Philister
Ein Kerl mit viel Haar. Samson, so hiess doch der Mister.
Er hat eine Fee namens Delilah geritten,
Die hat ihm sodann die Haare geschnitten.
Jetzt stehen sie alle nur noch in einem alten Register.

5

Registerharmonisierung

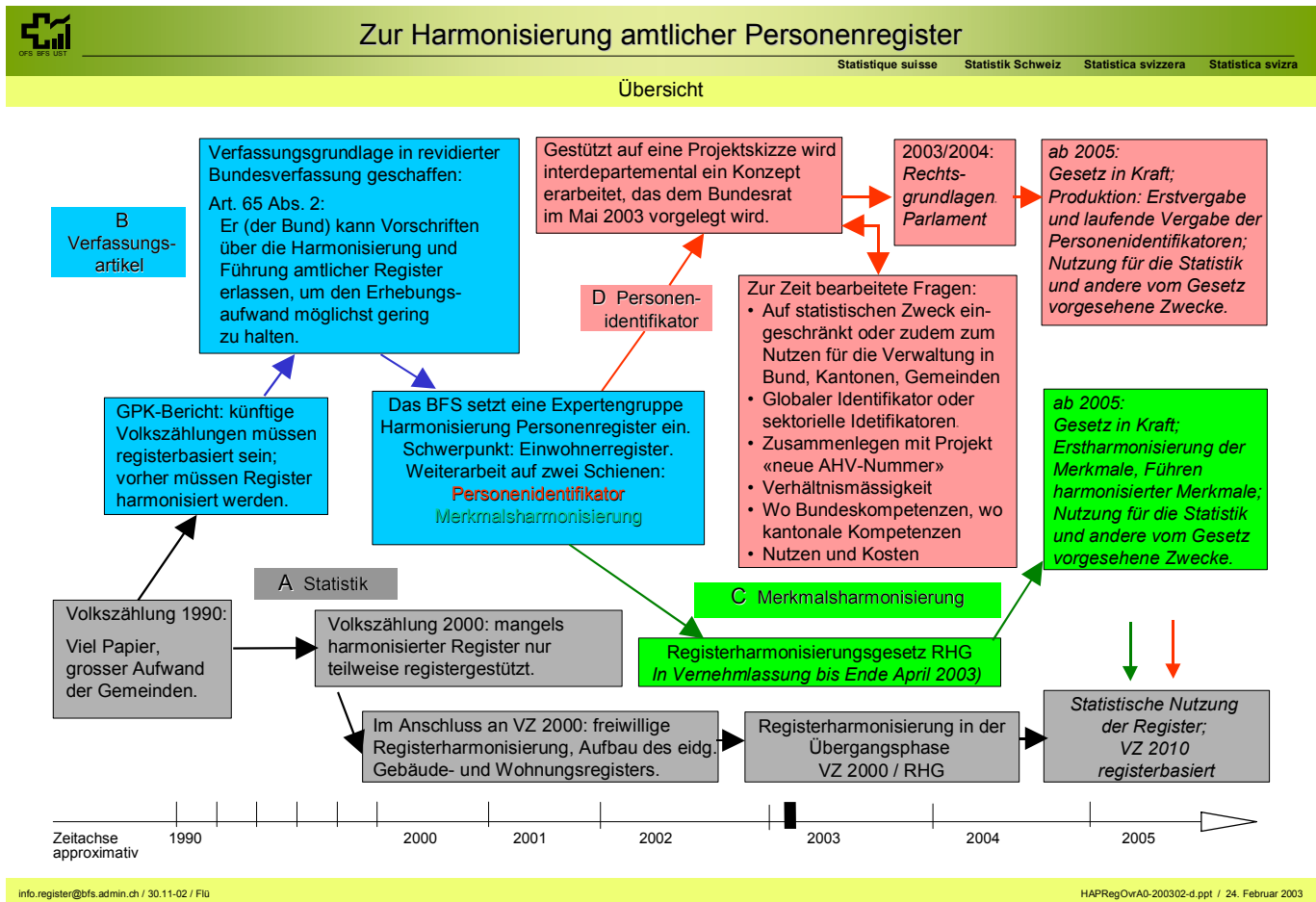
Harmonisierung amtlicher Personenregister

Ein interessanter und spannender Vortrag. Frau D. Spahn und Herr D. Ullmann vom eidg. statistischen Amt stellten anlässlich der GV des ISACA Switzerland Chapters vom 28. März 2003 in Bern die Situation der Harmonisierungsbestrebungen des Bundes bei den Personenregistern vor. Die nachfolgende Übersicht zeigt Inhalt und Zeitplan. Ausgangspunkt war der „Papierkrieg“ anlässlich der Volkszählung 1990, als die Geschäftsprüfungskommission des Nationalrates eine effizien-

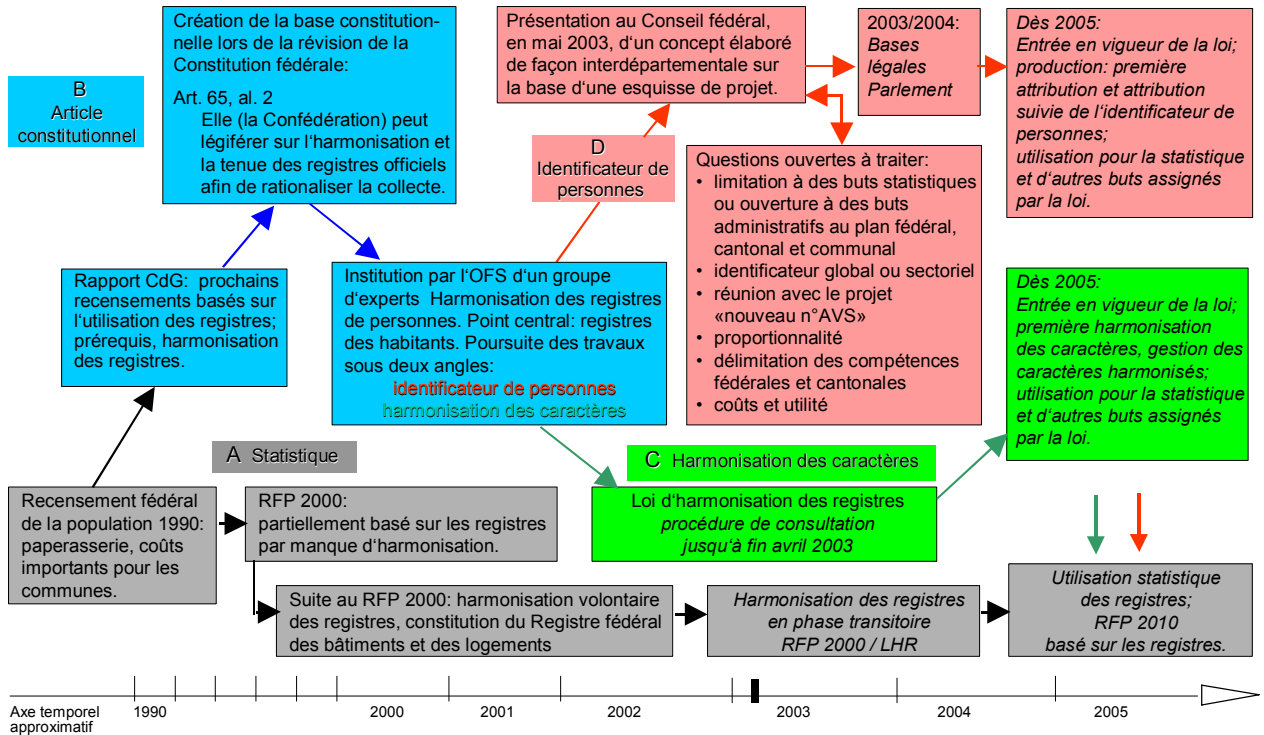
tere Abwicklung der Prozedur verlangte. Im Vordergrund stehen einerseits die Harmonisierung der Register (und Registernummern) bei der Einwohnerkontrolle, den Sozialämtern, den Transportinstitutionen etc., andererseits die Vereinheitlichung der Merkmalskennzeichen.

Gezwungenermassen ergaben sich bei den Bestrebungen zur Vereinheitlichung Konflikte mit den Interessen des Datenschutzes, die teilweise noch zu lösen sind. Die angeregte

Diskussion ergab übrigens, dass auf internationaler Ebene verschiedene Länder ansatzweise oder gar generell (z.B. Finnland) Lösungen in dieser Richtung aufweisen, dagegen zwischenstaatlich (weder europäisch noch global) keine Harmonisierung vorgesehen ist.



Harmonisation des registres officiels de personnes
Aperçu



Registerharmonisierung

Identifier Fritz Müller pour mieux le protéger !

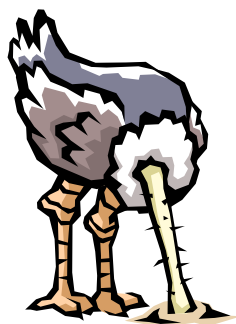
Nous avons tous été un jour ou l'autre confrontés à ces fastidieuses recherches de personnes présentant des noms trop communs en Suisse. Nous avons alors rêvé de disposer d'un numéro personnel fiable qui permette d'être sûr que le Fritz Müller inscrit au Registre du Commerce comme administrateur de la Müller AG est bien le Fritz Müller dont l'Office des Poursuites a par exemple établi l'extrait qui mentionne un nombre impressionnant de poursuites ouvertes...

Le numéro AVS n'est pas à même de remplir cette fonction d'identification. Il change en cas de naturalisation, de mariage et de changement de sexe. Le numéro idéal devrait être bâti sur deux bases : celles des annonces de l'Etat-civil pour les personnes nées en Suisse et celles des entrées en Suisse pour les autres.

Réjouissez-vous : ce projet existe ! Conduit par l'Office fédéral de la statistique, il devrait permettre d'attribuer un numéro personnel unique sur la base de 5 informations : nom, prénom, sexe, date et lieu de naissance. Une idée simple mais qui permettrait de simplifier toutes les démarches administratives. Selon un des processus envisagés, Monsieur Müller adresserait son changement d'adresse au Contrôle des habitants de sa commune de départ, qui transmet cette informa-

tion au fichier central pour qu'il la retransmette à toutes les administrations qui lui ont une fois demandé le numéro personnel de Monsieur Müller. Le fichier central n'enregistre donc aucune autre donnée que les 5 informations nécessaires à l'identification et les administrations « intéressées » au suivi de Monsieur Müller. Tous les échanges seront effectués sous forme chiffrée et les exigences prévues dans la législation sur la protection des données seront respectées.

Tout va donc bien ? Non bien sûr... L'Office fédéral de la statistique devra se battre contre de nombreux défenseurs de la protection des données qui s'opposeront à ce projet sans même s'être donné la peine de le comprendre. La seule idée d'un numéro personnel unique leur fait peur et entraînera leur « veto ».



Il nous appartiendra – chers lecteurs qui êtes à même de saisir la portée d'un tel projet – de soutenir ce projet. Il faudra notamment rappeler :

- que celui-ci ne créera aucune base légale pour de nouveaux échanges de données,
- que les comparaisons « sauvages » de données (matching) se déroulent déjà aujourd'hui, avec ou sans numéro personnel,
- que la vraie défense de la personnalité passe par des audits réguliers (également dans le secteur privé !) afin de vérifier que les exigences légales sont respectées et non par le chaos informatique,
- que des sommes astronomiques sont gaspillées chaque année en Suisse pour la gestion de données de base des personnes, comme les adresses ou les changements de nom,
- que la grande majorité des citoyens attendent de leurs administrations qu'elles collaborent entre elles. Ils apprécient par exemple lorsque les cantons se transmettent spontanément les informations après un déménagement, évitant ainsi aux particuliers de devoir remplir une montagne de formulaires.

Enfin, n'oublions pas que l'Histoire nous apprend que pour bien les protéger, il est indispensable d'identifier correctement les personnes. La fameuse affaire des fiches du Ministère public de la Confédération avait par exemple eu des conséquences dramatiques : des personnes avaient été licenciées car leur employeur les avait confondues avec un homonyme présentant un passé de terroriste ! De telles erreurs montrent que le chaos actuel n'est pas non plus sans risques...

Michel Huissoud, Vice-président

Registerharmonisierung

Die registrierte Gesellschaft

Die registrierte Gesellschaft

Das eidgenössische Departement des Innern hat den Entwurf des *Bundesgesetzes über die Harmonisierung der Einwohnerregister und anderer amtlicher Personenregister* in die Vernehmlassung gegeben. Es ist einzusehen, dass das Gesetz für Erbsenzähler eine wichtige Angelegenheit ist. Dennoch bin ich der Ansicht, dass man sich teilweise Illusionen hingibt. Ich kann mir deshalb nicht verklemmen, einige bissige Kommentare abzugeben.

Der gläserne Mensch

Als ich zum erstenmal Orson Welles' *1984* las, war ich einerseits noch sehr jung und von den Zukunftsvisionen des Utopisten beeindruckt. Als 1984 dann vorbeikam, war ich einerseits erleichtert zu sehen, was alles nicht Tatsache geworden war, und andererseits beunruhigt, in welcher Richtung sich die Gesellschaft eben doch bewegt. Das vorliegende Gesetz ist m.E. ein weiterer Schritt, dass wir uns total registrieren, klassieren und letztlich überwachen lassen.

Der Clochard

Glücklicherweise hat es bisher immer wieder Individuen gegeben, die sich in ihrer Originalität den Regeln der Behörden zu entziehen

wussten. Werden sie mit der neuen Harmonisierung nun endgültig in die Illegalität verbannt? Sind Fahrende und Zigeuner heute schon dort? Ich nehme an, es gibt diese Leute in Zukunft offiziell gar nicht. Und was ist mit den illegal eingewanderten/ eingeschleppten Ausländern? Erhalten sie, wie mein Clochard, in nicht allzu ferner Zukunft keine ärztliche Betreuung mehr, weil sie im Spital keine „eindeutige Personenidentifikationsnummer“ vorweisen können? Art. 5 (Vollständigkeit) des Gesetzesentwurfes ist wohl eine Illusion.

Der Zwitter und das Neutrum

Wie doppelgeschlechtliche Wesen „verarbeitet“ werden, ist mir schleierhaft. Wahrscheinlich haben sie sich eindeutig für das eine oder andere Geschlecht zu entscheiden. Geschlechtsumwandlungen dürften bei der neuen Personennummer wohl etwa ebenso leicht zu behandeln sein, wie Heiraten und Scheidungen heute.

Der verlorene Sohn und die verschollene Tochter

Es soll vorkommen, dass sich Personen aus Haushalten entfernen, ohne sich ordnungsgemäss beim Haushaltsvorstand, geschweige denn beim Einwohnermeldeamt abzumelden. Sind sie für das System „gestor-

ben“? Was passiert, wenn sie nach ihrem Abenteuer in Südostasien mit Zwillingen wieder auftauchen? Gehen sie in Quarantäne, bis ihre Personalnummer reaktiviert ist und der Nachwuchs ordnungsgemäss registriert? Hoffentlich streikt dann das Datenerfassungspersonal nicht allzu lang.

Wenn schon, denn schon

Die Harmonisierung scheint sich (so lese ich den Gesetzesentwurf wenigstens) auf natürliche Personen, Haushalte und Katasterinhalte (Gebäude etc.) zu beschränken. Warum werden juristische Personen nicht explizit erwähnt? Weil sie kein Geschlecht haben? Geburt und Tod kennen sie ja. Warum werden Handelsregister nicht ebenfalls mit diesem Gesetz „harmonisiert“? Wie steht es mit juristischen Personen, die nicht im Handelsregister eingetragen sind?

Warum werden die (wohl eidgenössisch geführten) Personenregister der Armee, der AHV/IV, des Zivilschutzes, usw. nicht ebenfalls „harmonisiert“?

Der arme Datenschutzbeauftragte und der ebenso arme Informatik-Revisor

Die Beteuerungen, das Datenschutzgesetz müsse eingehalten werden, hält nicht von der Erkenntnis ab, dass viele personenbezogene Daten gespeichert werden können und auch werden, deren Verwendung letztlich einzelnen Datenbaronen vorbehalten

bleibt. Es wird immer wieder Möglichkeiten geben, die Daten zu verwenden und zu missbrauchen. Das beste IKS kann dies kaum verhindern. Die besten Absichten werden einen Fall „Belasi“ (in übertragenem Sinne auf dem Gebiet des Datenschutzes) nicht zu verhindern wissen, wenn Daten systematisch und umfassend gesammelt und gespeichert werden. Wer trägt die Verantwortung bei einer Panne? Ist sie allenfalls überhaupt wieder gutzumachen?

Der politische Fehltritt

Ohne polemisch zu werden: Der Hinweis auf eine „Europakompatibilität“ im ersten und einleitenden Abschnitt der Vernehmlassungsschrift stört mich. Insbesondere, als internationale Vereinheitlichungsbestrebungen angeblich fehlen. Heulen wir auch hier mit den Wölfen?

Max F. Bretscher, CINE

Datenschutz

Datenschutz im Data Warehouse

Vor dem Hintergrund der derzeit schwachen wirtschaftlichen Situation weltweit und rückläufigen Umsätzen vieler Unternehmen stellt sich vermehrt die Frage, wie bestehende Kundenbeziehungen weiter ausgebaut bzw. aktiviert werden können oder die Unternehmenssteuerung verbessert werden kann. Um dies zu erreichen, benötigt man möglichst umfassendes Wissen bzw. Daten über das eigene Unternehmen. Dies führt direkt zur Etablierung eines Data Warehouses, das die Informationsbedürfnisse möglichst aller im Unternehmen befindlicher Bereiche abdecken soll. Hierzu müssen umfangreiche Daten aus allen Bereichen des Unternehmens gespeichert und historisiert sowie entsprechende Mechanismen zur Auswertung und somit Nutzung dieser Daten eingerichtet werden. An diesem Punkt stellt sich natürlich die Frage, ob es zulässig ist, umfangreiche Daten zu sammeln und auszuwerten oder ob es Einschränkungen bei der Sammlung oder Auswertung dieser Daten gibt. Grundsätzlich kann man sagen, dass der gesetzliche Datenschutz die Erhebung, Verarbeitung (diese beinhaltet u.a. auch die Speicherung von Daten) und Nutzung von personalisierten Daten reglementiert.

Grundgedanken zur Konzeption

Bei der Ausgestaltung eines Data Warehouses gibt es unterschiedliche Vorgehensweisen, die Daten hinsichtlich ihrer Detailtiefe bzw. Aggregation und ihres Umfangs zu betrachten. Je nach künftigem Einsatzzweck kann es sich bei den Daten im Data Warehouse um ausschließlich aggregierte oder Daten auf Basis einzelner Datensätze aus den Vorsystemen handeln. Eine Kombination beider Formen ist in der Praxis häufig anzutreffen. Da hier bereits der Grundstein für datenschutzrelevante Sachverhalte gelegt wird, sollten die im folgenden diskutierten Fragestellungen bereits bei der Konzeption des Data Warehouses sowie bei späteren Erweiterungen bzw. Veränderungen berücksichtigt werden. Hierbei sollte auch die Frage nach der Notwendigkeit der Sammlung der Daten vor dem Hintergrund der verfolgten Auswertungsziele gestellt werden. Denn die sogenannte Vorratsdatensammlung wirft nicht nur datenschutzrechtliche Probleme auf, sondern stellt die IT-Abteilung häufig auch vor technische oder Ressourcenprobleme, die letztlich in der Regel mit inperformanten Systemen und somit unzufriedenen Nutzern enden.

Datenschutz in Deutschland

Da es keine konkreten rechtlichen Regelungen zum Datenschutz im Data Warehouse gibt, werden zur datenschutzrechtlichen Beurteilung von Data Warehouse Systemen die allgemeineren Rechtsquellen des Bundesdatenschutzgesetzes (BDSG) sowie ergänzend die spezialgesetzlichen Regelungen zum Datenschutz, z.B. das Teledienstedatenschutzgesetz (TDDSG), angewandt. Der Datenschutz nach deutschem Recht dient dem Schutz der persönlichen Daten einer jeden natürlichen Person und soll ihr ein Selbstbestimmungsrecht über ihre persönlichen Daten einräumen. Ein genereller Grundsatz ist das Gebot der Datenvermeidung und der Datensparsamkeit, das in § 3a BDSG erwähnt ist, und allen Unternehmen das Ziel vorgibt, so wenig wie nötig personenbezogene Daten zu erheben, zu verarbeiten und zu nutzen. Dieser Grundsatz ist von jedem Unternehmen bei der Konzeption oder Auswahl von Datenverarbeitungssystemen zu berücksichtigen. Das Data Warehouse stellt in diesem Zusammenhang ein mögliches Datenverarbeitungssystem dar.

Datenspeicherung im Data Warehouse

Die Datenspeicherung im Data Warehouse ist die erste datenschutzrechtliche Hürde, um überhaupt an die Nutzung der Daten denken zu können. Solange keine personalisierten Daten wie z.B. Kundendaten oder Personaldaten im Data Warehouse gesammelt werden sollen, ist die Datenspeicherung zulässig. Prob-

lematisch wird es erst, wenn genau diese Daten für die spätere Nutzung im Data Warehouse enthalten sein sollen. Zuerst sollen nachfolgend die unterschiedlichen Möglichkeiten der Datenspeicherung nach BDSG betrachtet werden, angefangen bei der Anonymisierung bzw. Pseudonymisierung der Daten bis hin zu personalisierten Einzeldatensätzen.

Die Anonymisierung bzw. Pseudonymisierung der Daten ist ausdrücklich im BDSG § 3a vorgesehen und als datenschutzkonforme Möglichkeit der Datenspeicherung aufgeführt. Wie sieht es aber mit der Speicherung personalisierter Daten aus? Grundsätzlich ist hier festzustellen, dass diese Form der Datenspeicherung nach BDSG nicht zulässig ist. Es gibt jedoch drei Fälle nach § 28 Abs. 1 BDSG, in denen eine Speicherung von personalisierten Daten zulässig ist:

1. Wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient.
2. Soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.
3. Wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

Da häufig über die Zweckbestimmung des Vertrages hinaus Daten gespeichert und genutzt werden sollen und diese Daten auch nicht allgemein zugänglich sind, ist oft eine entsprechende Abwägung der berechtigten Interessen des Unternehmens gegen die schutzwürdigen Interessen des Betroffenen durchzuführen. Das Ergebnis dieser Abwägung sollte möglichst objektiv und unabhängig im Unternehmen geprüft werden, bevor es zu einer Umsetzung kommt.

Fallen die erhobenen Daten bspw. unter das TDDSG, so ist nur eine Speicherung von zwingend notwendigen Bestandsdaten oder Nutzungsdaten, die für die Abrechnung eines Dienstes notwendig sind, zulässig. Alle anderen Nutzungsdaten aus dem Teledienst müssen grundsätzlich nach Beendigung dieses Dienstes gelöscht werden oder dürfen gar nicht erst gespeichert werden. Somit ergeben sich aus dem TDDSG noch strengere Anforderungen an die Speicherung der Daten als aus dem BDSG.

Wo liegt nun aber die Abgrenzung zwischen Daten, die unter das BDSG fallen, und den Daten, die unter das TDDSG fallen? Eine plausible Abgrenzung, die von Peter Schaar in seinem Buch „Datenschutz im Internet“ vorgestellt und erläutert wird, stellt ab auf einen sogenannten „Online-“ sowie einen „Offline-Bereich“. Demnach fallen auch über einen Teledienst wie das Internet abgewickelte Geschäfte, die lediglich eine ebenso in der Offline-Welt vorhandene Transaktion abbilden, in den sogenannten „Offline-Bereich“. Für das TDDSG relevant sind jedoch

nur alle Online-Fälle, die Offline-Fälle hingegen werden nach dem BDSG behandelt.

Zur näheren Erläuterung dieser Abgrenzung soll hier ein kurzes Beispiel angeführt werden:

Im Rahmen des Online Banking stellt das Ausführen einer Überweisung im Internet einen typischen Offline-Fall dar. Im Gegensatz dazu wären Nutzungsdaten aus dem Abruf frei verfügbarer Finanzinformationen aus dem Internet ein typischer Online-Fall, da diese Aktion keinem typischen Kundengeschäft in einer Bankfiliale entspricht.

Bis jetzt haben wir über aktive Kundenverbindungen gesprochen, aber wie verhält es sich mit Ex-Kunden oder Personen, die Interesse an einem Produkt bekundet haben, jedoch nie Kunde geworden sind? Grundsätzlich dürfen diese Daten nicht mehr im Data Warehouse in personalisierter Form enthalten sein. D.h. um beim Beispiel der Ex-Kunden zu bleiben, müssten alle Daten eines Ex-Kunden nach Beendigung der Geschäftsbeziehung gelöscht oder anonymisiert werden. Bei einer Löschung, Anonymisierung oder Pseudonymisierung dieser Daten sind jedoch weitere Vorschriften, wie z.B. Aufbewahrungsvorschriften, zu berücksichtigen. Eine andere Möglichkeit könnte in der Kenntlichmachung des Status als Ex-Kunde durch das Setzen eines Kennzeichens liegen, wodurch diese Daten bei späteren Auswertungen auf Basis von personalisierten Kundendaten nicht mehr mit einbezogen werden dürfen. Wichtig ist in diesem Zusammenhang die

Etablierung klarer Regelungen und Anweisungen zur Nutzung dieser Daten, da Auswertungen trotz Kennzeichnung natürlich weiterhin möglich sind. Diese Vorgehensweise entspricht nicht vollständig dem niedergelegten Datenschutzgedanken, da die personalisierten Daten weiterhin vorhanden sind, und kann somit lediglich als Notlösung betrachtet werden.

Nutzung von Daten

Wenn die Frage der Datenspeicherung geklärt ist und entsprechende Daten im Data Warehouse vorhanden sind, ist im nächsten Schritt die Frage der zulässigen Nutzung dieser Daten zu klären.

Werden die gesammelten Daten im Data Warehouse lediglich für anonymisierte Analysen verwendet, so ist dies nach BDSG wie auch nach TDDSG zulässig. Problematisch wird die Nutzung der personalisierten Daten oder auch der pseudonymisierten Daten, wenn nach der Analyse die Verbindung mit den Personendaten wieder hergestellt und etwaige Rückschlüsse gezogen werden. Dies kann nur dann zulässig sein, wenn keine schutzwürdigen Interessen des Kunden am Ausschluss der Verarbeitung oder Nutzung die berechtigten Interessen des Unternehmens an der Verarbeitung oder Nutzung überwiegen. Sollte der Kunde durch eine derartige Nutzung schlechter gestellt werden als zuvor, so könnte ein schutzwürdiges Interesse seinerseits am Ausschluss der Nutzung vorliegen, dass das berechnete Interesse des Unternehmens überwiegen könnte.

Auch hierzu soll ein kurzes Beispiel gegeben werden:

Sollte beispielsweise ein Bankkunde gekündigt werden, da eine Analyse seiner Nutzungsdaten ergeben hat, dass Kunden mit seinem Profil ein besonders hohes Betrugspotential bergen, so könnte dies unzulässig sein. Dies könnte sich daraus ergeben, dass dieser Kunde aufgrund einer Auswertung aus dem Data Warehouse mit Bezug zu und unter Nutzung seiner Personendaten (ohne seine Einwilligung) schlechter gestellt wird als zuvor.

Möchte ein Unternehmen ohne jedwede Restriktionen die Daten eines Kunden im Data Warehouse speichern und nutzen, so gibt es lediglich die Möglichkeit, dies über eine Einwilligung des Kunden in die Speicherung und Nutzung nach § 4a BDSG bzw. bei Telediensten nach § 3 TDDSG zu erreichen. Gegenstand dieser Einwilligung ist die vorab zu erfolgende umfassende Information des Kunden nach § 4 Abs. 1 TDDSG über die Verarbeitung seiner Bestands- und Nutzungsdaten. Bei der Konzeption des Data Warehouses muss auch der Fall berücksichtigt werden, dass ein Kunde diese Einwilligung nicht erteilt. Hierfür muss ein entsprechendes Kennzeichen vorhanden sein, um diese Datensätze von etwaigen Aktionen auszunehmen.

Die Nutzungsprofile dürfen ausschließlich in pseudonymisierter Form für die im § 6 Abs. 3 TDDSG genannten Zwecke, d.h. für die Werbung, Marktforschung oder zur bedarfsgerechten Gestaltung der Dienste, verwendet werden, wenn

keine weitere Einwilligung durch den Kunden vorliegt. Somit dürfen die Daten aus dem Nutzungsprofil bspw. nicht zur Bonitätsprüfung eines Kunden herangezogen werden.

Data Mining

Generell gilt das Thema Data Mining in Verbindung mit personenbezogenen Daten bei Datenschützern als nicht mit dem Datenschutz vereinbar, da das Data Mining dem Auffinden neuer, bisher nicht bekannter Beziehungen zwischen den vorhandenen Daten dient. Grundlage der Nutzung von Daten unter Berücksichtigung des Datenschutzes ist jedoch, dass diese nur für einen im Voraus durch die Vertragsbeziehung zwischen Kunde und Unternehmen bestimmten und bekannten Zweck genutzt werden dürfen. Dieser ist jedoch zum Zeitpunkt eines Vertrages mit dem Kunden oder einer Einwilligung noch nicht bekannt.

Handelt es sich um nicht personenbezogene, also pseudonymisierte oder anonymisierte, Daten, so spricht auch aus Sicht des Datenschutzes nichts gegen den Einsatz von Data Mining, da es sich in diesem Fall nicht mehr um personalisierte Daten handelt.

Verfahrensverzeichnis

Um die Transparenz der Verarbeitung von datenschutzrechtlich relevanten Daten für Außenstehende zu erhöhen, ist mit § 4g BDSG das sogenannte Verfahrensverzeichnis eingeführt worden, das von jedem Unternehmen erstellt und auf An-

frage zur Verfügung gestellt werden muss.

Eine der Kernfragen ist, welche Angaben in diesem Verfahrensverzeichnis enthalten sein müssen. Dies ist in § 4e BDSG aufgeführt und umfasst neben Angaben zur Firma, die Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung, betroffene Personengruppen und zugehörige Daten, Empfänger der Daten, Regelfristen zur Löschung der Daten, geplante Datenübermittlung in Drittstaaten sowie Beurteilung der Maßnahmen nach § 9 BDSG zur Gewährleistung der Verarbeitungssicherheit.

Risiken und Folgen aus Verstößen

Die Nichtbeachtung der Datenschutzanforderungen nach BDSG bzw. TDDSG ist mit unterschiedlichen Risiken verbunden, die hier lediglich kurz aufgeführt werden sollen. Eine Bewertung dieser Risiken muss letztlich in der Regel durch das Management getroffen werden, insbesondere wenn bewusst Grauzonen oder Grenzfälle betrachtet werden.

Folgende Risiken und Folgen ergeben sich:

1. Bußgeld: Aus § 43 BDSG kann sich ein Bußgeld von bis zu T€ 250 bei der Nichtbeachtung von Datenschutzvorschriften nach BDSG ergeben. Nach § 9 TDDSG kann eine Ordnungswidrigkeit mit einem Bußgeld von bis zu T€ 50 geahndet werden.
2. Freiheitsstrafe: Nach § 44 BDSG kann bei vorsätzlichen Handlungen

gegen Entgelt oder in der Absicht, sich zu bereichern oder einen anderen zu schädigen, bei einigen Tatbeständen aus dem o.g. § 43 BDSG auch eine Freiheitsstrafe bis zu zwei Jahren verhängt bzw. eine weitere Geldstrafe erhoben werden. Eine solche Tat wird jedoch ausschließlich auf Antrag der Betroffenen, der verantwortlichen Stelle, des Bundesbeauftragten für den Datenschutz oder der Aufsichtsbehörde verfolgt.

3. Änderungen: Abgeleitet aus einem festgestellten Verstoß gegen Datenschutzvorschriften (s. 1.) dürfte es zu der Auflage kommen, dass entsprechende Veränderungen vorgenommen werden müssten, um die Anforderungen zu erfüllen.

4. Imageschaden: Das wahrscheinlich schwerwiegendste Risiko ist der Imageschaden, der aus dem Bekanntwerden der Nichtbeachtung von Datenschutzvorschriften resultieren kann. Ein hieraus entstehender Schaden ist kaum im Voraus bezifferbar.

Die oben aufgeführten Fälle 1 und 3 werden wahrscheinlich immer zusammen eintreten, aber auch der Fall 4 könnte sehr wahrscheinlich in Kombination mit den beiden Fällen 1 und 3 eintreten. Der Fall 2 dürfte eine äußerst seltenen Ausnahme sein, da eine entsprechende Verfolgung auch erst auf Antrag eingeleitet wird.

Fazit

Das Themengebiet des Datenschutzes in Verbindung mit einem Data Warehouse wird noch immer sehr konträr diskutiert und birgt eine Menge Risiken, insbesondere wenn der Datenschutz nicht bereits bei der Konzeption eines Data Warehouses

mit bedacht worden ist. Viele Datenschützer lehnen das Data Warehouse bereits grundsätzlich ab, aber es gibt auch Möglichkeiten und Wege, ein Data Warehouse datenschutzkonform zu konzeptionieren und zu betreiben. Eine Grundüberlegung bei der Konzeption und Realisierung des Data Warehouses sollte sein, welche Daten für die angedachte zukünftige Nutzung wirklich benötigt werden. Häufig herrscht die Meinung vor, alle im Unternehmen vorhandenen Daten zu sammeln und zu historisieren. Dies macht aus Kosten- und Performancegründen häufig wenig Sinn und wirft insbesondere bei Kunden- oder Personaldaten eine Menge datenschutzrechtliche Probleme auf.

Somit kann die Empfehlung nur lauten, vor der Realisierung eines Data Warehouses datenschutzrechtliche Belange in die Planung mit aufzunehmen und die zukünftige Nutzung und dafür notwendige Daten, auch vor dem Hintergrund der Speicherung ausschließlich relevanter Daten, zu durchdenken und festzulegen.

Ingo Struckmeyer

Datenschutz

Some Provocative Thoughts on Data Protection

Many ancient stories seem to imply that once upon a time people were proud of their good reputation. They had an interest of this image to be spread. Along came data protection. And all of a sudden I get the impression that it is society's duty to cover up the ill reputation of villains and culprits.

I observe quite often the misuse of the noble attempts to establish data protection and guarantee some type of privacy to the individual. Included are the covering up of dangerous contagious diseases, such as HIV, the nondisclosure of wrongdoings (that are not necessarily recorded by law), the burning of underlying evidence in order to qualify as "paperless person" seeking asylum, but probably also some aspects of the legendary Swiss bank secret and maybe also the canonical confession secret. Agreed: Probably everyone has weak points that she or he is not very proud of, but even if the facts maybe shameful: I profess that truth has never hurt anyone.

What then is the legitimate concern of data protection? Steven J. Ross claims in his article *Privacy Parts* in Volume 6/2002 of the *Information Systems Control Journal* on this score that he fails to find a suitable definition. Well, we have to admit that every nation, society or community has its proper understanding of privacy. The line where common

interest overrules individual concerns is not everywhere the same. Neither is the understanding of what is right and wrong. We Westerners seem sometimes to forget that. But even here the joke about the understanding of law differs: "In England everything is allowed that is not forbidden; in Germany everything is forbidden that is not allowed; in Italy everything is allowed, even what is forbidden; and in Russia everything is forbidden, even what is allowed."

The differences in the basic concepts then seem to rule the definitions of data protection and privacy. That also explains why people who have been brought up under Roman law do not understand what those are talking about who have been living under Common law rules. We run into even further problems when we enter scenes of other religions, such as Islam, Hinduism, Buddhism or any view of the world that we conceitedly call "primitive". But we do not have to go that far: Communism in its basic traits (whether original arch-Christian or modern Marxist) violates the concept of data protection almost step by step.

Should we therefore capitulate before the ultimate question of data protection, confidence and privacy, saying with Frederic the Great: "Let everyone be happy in his own way"? Probably not.

I note that the topic of data protection has become an issue only with the advent of EDP. Before, nobody seemed to be really concerned about the huge amounts of data that had been accumulated in archives of churches, governments and private institutions. To the contrary: Students were happy to be able to dig into the treasures of times past. Many a historian and linguistic student would never have completed his PhD without the very personal recordings of famous and infamous people. However, this was information that had to be researched on an individual basis, and could not be retrieved systematically using a mechanical device. Nosing in other people's record (especially if they were dead) was tolerated, if not desired.

The conclusion is tempting that data protection is not really an issue of protecting data as such, but rather an issue of its abuse by electronic means. It is interesting to note in that connection that France addressed in its initial data protection act exclusively personal data in electronic form. I personally believe that the core of all data protection efforts must be the prevention of misuse of personal data.

For one, that is the concern that wrong information might be stored and therefore lead to erroneous conclusions. Hence, the right of the person concerned to have data corrected (or blocked). In order to exercise this right, the person concerned must have the right to inspect the data that is stored by the third party. Only if the person knows which data is stored, action can be

taken. Now that is quite a task for the organization storing the data. It is obvious that not everyone can be allowed to browse an entire data warehouse in order to find out whether personal data is stored. Rights of other persons might be violated by such a process. However, the organization storing the data must be in a position to positively answer any request by persons concerned: Such and such data is stored vs. no data is stored. Are the organizations you are working for in a position to truly answer this question?

Furthermore, the possibility to analyze and make use of data in such way that negative effects result against innocent individuals should be eliminated. That, however, is a task impossible to accomplish, I would claim, unless IT is abandoned completely. What to do? I presume that this question will worry jurists

for some time to come: It is impossible to define the content of data that should be protected as this quality might change over time. And the attempts to attack the problem through formalistic means have been futile so far according to my point of view- and probably will always be.

What remains as conclusion is the trivial insight that data protection results in the phrase: "Do with the data you accumulate what you feel free to do, but if caught doing harm to someone in the process, you are automatically guilty." Not very professional, and not very legally clean, either. But probably true in any kind of society.

Max F. Bretscher

Dringend: Termin 30. April 2003

CISA: Entwicklung von Multiple-Choice-Fragen

ISACA International sucht für das CISA Review Manual 2004 Personen, welche neue Multiple-Choice-Fragen in Englisch entwickeln. Interessenten wenden sich bitte in Englisch an:

Elia Fernández Torres, CISA
Manager-Certification Study Program And Educational
Development
Information Systems Audit and Control Association
3701 Algonquin Road Suite 1010,
Rolling Meadows, IL 60008, USA
Phone: +1.847.253.1545 ext.484
Fax: +1.847.253.1443
E-mail: efernandez@isaca.org

Konfliktmediation

Ein neues Berufsbild?

Einleitung

Sicherheitsbeauftragte, IT-Manager, externe Berater und Lieferanten: Sie alle laufen das Risiko, in eine Konfliktsituation zu geraten. Dies trifft z.B. dann ein, wenn sich ein Schadenfall ereignet, welchen die Auftraggeber nicht erwarteten. Fragen werden gestellt: „Warum wurden keine Maßnahmen getroffen?“ „Warum haben die Maßnahmen nicht ausgereicht?“ „Wo liegt die Verantwortung?“. Die ersten zwei Fragen mögen neutral sein, die dritte aber bewegt sich in Richtung Konflikt und ein Rechtsverfahren könnte vor der Tür stehen.

Auseinandersetzungen im Bereich Risikomanagement sind normalerweise keine leichten Konflikte. Die Thematik der Risiken und Sicherheit hat meistens abstrakten Charakter, wobei subjektive Einschätzungen eine übergeordnete Rolle spielen; Ziele und Erwartungen lassen sich aber schwierig quantifizieren. Zwischen Vertraggeber und Vertragsnehmer können sich damit schwierig zu glättende Konflikte ergeben, wo auseinandergehende Annahmen, Prämissen, Hypothesen und Einschätzungen dafür sorgen, dass jedermann Recht und Unrecht zur gleichen Zeit hat.

Konflikte entstehen grundsätzlich, wenn ein Auftraggeber mit der Rendite seiner Investitionen unzufrieden ist. Was zum Beispiel, wenn ein

Sicherheitsunternehmen bei einem Auftraggeber eine Alarmanlage installiert hat, die durch ein anderes Sicherheitsberatungsbüro empfohlen wurde? Durch eine Unvollkommenheit im System findet trotzdem ein Einbruch mit erheblichen Direktschäden und Folgeschäden statt. Das Sicherheitsunternehmen behauptet steif und fest, dass das System vorschriftsgemäß installiert wurde und ordnungsgemäß funktioniert hat. Das Sicherheitsberatungsbüro wittert die Zuschreibung einer Schuld und zweifelt die Meinung des Sicherheitsunternehmens an. Es deutet gleichzeitig an, dass der Auftraggeber es unterlassen hat, bestimmte wichtige Information zur Verfügung zu stellen. Der Auftraggeber spielt den Ball wieder zurück mit der Begründung, dass er nicht ohne Grund ein Sicherheitsberatungsbüro eingesetzt hat, dass das Sicherheitsberatungsbüro eine mangelhafte Risikoanalyse durchgeführt hat, usw. Jetzt ist jeder böse auf jeden und es zeichnen sich Konturen eines langwierigen und kostspieligen Prozesses ab.

Ähnliche Abläufe sind vorstellbar für EDV-Bereiche: Eigenentwicklungen und Paket-Implementationen, die Verzögerungen erleiden oder eine beschränkte Funktionalität aufweisen, outgesourcete Dienstleistungen, deren Service Levels nicht eingehalten werden, oder wo die Interpretationen der zu liefernden Leistungen weit auseinanderlaufen. Fehlinterpretationen, Unkenntnis, Unerfahren-

heit und Versagen sind immer da, wo Menschen planen und arbeiten sowie Vereinbarungen zwischen ihnen zustande kommen.

Wenn sich der Berater oder Lieferant vertraglich ungenügend gegen seine gesetzliche Haftpflicht abgesichert hat, könnte sich auf den ersten Blick ein gerichtliches Verfahren für die Auftraggeber bezahlt machen. Doch auch wenn vertraglich abgesichert, sollten sich Berater oder Lieferant überlegen, ob sie unversehrt davon kommen. Jede Klage kostet Zeit, Geld, und ist letztlich kontraproduktiv. Es kommt aber nicht immer, wie es kommen sollte; es gibt manchmal Lösungen, die effektiver und weniger destruktiv für die Beziehung sind. Übrigens, wo kein Kläger ist, ist kein Richter...

Sinn der Mediation

Wenn Parteien ihre Konflikte nicht selbständig lösen können – je größer die Belange sind, desto schlechter stehen die Chancen dazu – droht eine gerichtliche Auseinandersetzung und damit wird die Kontrolle über das Projekt allen Parteien entzogen. Daher wächst seit einigen Jahren die Beliebtheit der Mediation im EDV-Bereich.

Mediation heißt zwischen kämpfenden Parteien vermitteln und ist eigentlich nichts Neues. Seit Jahrhunderten ist die Vermittlung eines der wichtigsten Instrumente der Diplomatie. Konsenskünstler wie die UNO zeigen, daß Vermittlung und Kompromisse effektive (zwar nicht immer schnelle) Konfliktlösungs-

mechanismen sind. Aber: Wer nicht (mehr) redet, führt Krieg.

Wenn das Bewußtsein/die Anerkennung da ist, dass man einander braucht, oder sich immer wieder begegnen wird, können Parteien versuchen, ihre Konflikte unter Begleitung eines Mediators kooperativ und produktiv zu lösen.

Gerade bei komplexen Konflikten oder Konflikten in Bereichen, wofür spezifische Kenntnisse erforderlich sind, ist Mediation nicht nur eine effektive, sondern auch eine effiziente Art, Konflikte zu lösen. Im Bereich Risikomanagement wird die inhärente Komplexität durch den subjektiven Charakter von sowohl Risikoeinschätzungen als auch dem Maß, mit welchen Maßnahmen Risiken reduzieren, erhöht. In solchen Fällen handelt es sich um nicht erwartete Ereignisse und die wahrscheinlichen Folgeschäden.

Hinterher weiß man alles besser und es lässt sich nur noch schwierig herausfinden, welche Maßnahmen einen Unfall oder Vorfall unter welchen Umständen nach hätten vermeiden können. Die Chance auf eine schleunige Lösung wird damit niedrig, die Chance auf hohe Kosten wird dagegen groß und enge Freunde wird man hinterher auch nicht mehr sein.

Wenn Parteien unversöhnlich sind, nichts zur Sache tun und emotionale Spannungen einbringen, wird der Streit sich in eine andere Richtung bewegen. Vernünftige Verhandlungen werden nicht mehr möglich sein, weil sich die Positionen verhärten. Letztendlich übergeben die Parteien

die Kontrolle über ihre Lage in einem Prozessverfahren einem Dritten: Die Behörde oder ein Arbitragehof werden angerufen. Dort wird sich herausstellen, daß gesetzliche Regeln manchmal wichtiger sind als das Recht an sich. Von der Vernunft schon ganz zu schweigen.

Der Einsatz von Mediation bezieht sich auf Konflikte zwischen Unternehmen. Häufig geht es um die Frage, wie ein Vertragswerk interpretiert werden soll. Voraussetzung für erfolgreiche Mediation ist dabei ein gewisses Maß an allseitigem Vertrauen.

Mediation macht nur Sinn, wenn bestimmte Forderungen da sind.

Das Wesen der Mediation

Mediation kennzeichnet sich durch die folgenden Aspekte:

- Der Einsatz einer neutralen Person, welche die Parteien bei der Konfliktlösung unterstützt.
- Ein informelles und nichtöffentliches Verfahren, wo die Möglichkeit existiert, individuelle Gespräche zu führen.
- Die gemeinschaftliche Ausarbeitung von Problemlösungen und Evaluierung von Lösungsalternativen.
- Die Entscheidung bleibt in den Händen der Parteien.
- Die Übereinstimmung wird in einem rechtsgültigen Dokument festgelegt.

Mediation hat ihre Grenzen

Mediation bietet keine Lösung für Haftungskonflikte und Schadenersatzforderungen. Wenn ein offensichtlicher Fehler oder ein deutliches Fehlverhalten vorliegen, wird, wenn sich kein friedlicher Vergleich anbietet, nur die Arbitrage oder ein Rechtsverfahren die Antwort geben können. Auch bietet Mediation keine Lösung oder Kompensation für eine schwache oder eindeutige Rechtsposition.

Mediation wird scheitern, wenn Parteien die typischen Charakteristika eines Konfliktverhaltens zeigen. Typische Charakteristika von Konfliktverhalten beinhalten den Glauben, dass eine Partei Schuld hat, und die andere nicht. Damit geht die Überzeugung einher, dass dies so offensichtlich ist, dass ein Sieg fast garantiert ist. Lediglich juristische Auswirkungen werden betrachtet; andere Umstände sind sekundär. Die Blickrichtung dabei ist die Vergangenheit: Wer hat was wann gesagt, zu wem, und welche Konsequenzen die Vergangenheit auf die heutige (Rechts-)Position hat. Das eigentliche Ziel wird vergessen und durch ein neues ersetzt: Ein Neuanfang, wo jeder (hoffentlich) von seinen Fehler gelernt hat und wo Projekte nicht mehr fehlschlagen. In dem Moment, wo gerichtliche Schritte unternommen werden, ist die Mediation vorbei.

Bei Prozessen im Bereich fehlgeschlagener Projekte, IT-Investitionen oder -Beratungen wird ein Richter oder gesetzlicher Schiedsrichter ein Urteil über eine Angelegenheit

fällen, bei der er kein Spezialist ist. Nichts gegen die Kompetenz der Richter, aber sie müssen sich in so einem Fall auf den beschriebenen Sachverhalt verlassen, ohne „ins and outs“ zu kennen und zu verstehen, die Eigenheiten der Branche zu beherrschen und die nicht-juristische Aspekte im Vorfeld des Konfliktes in Erwägung zu ziehen. Ein Richterspruch konzentriert sich selten auf das eigentliche Problem, sondern basiert auf der juristischen Projektion des Verhaltens von Organisationen.

Ein richterliches Urteil schenkt Klarheit, bietet aber meistens keine Lösung für das ursprüngliche Problem. Zudem ist zu beachten, dass bei einem Urteilsspruch immer zumindest zwei Parteien betroffen sind. In den meisten Fällen werden die zuerkannten nur einen Teil der verlangten und als gerecht betrachteten Forderungen beinhalten. Das heißt in der Praxis, dass beide Parteien immer erhebliche Kosten und Unzufriedenheit mit als Endergebnis erhalten, und dass sie wieder von vorne beginnen können.

Gerade da liegt die Stärke der Mediation. Keiner weiß besser Bescheid über die Problematik, wie der Schaden entstanden ist, als die Parteien selbst. Sie müssen sich aber bereit erklären, den Scherbenhaufen aufzuräumen. Manchmal sollte man nach total andersartigen Lösungen suchen: Z.B. Kompensationen, neue Arten von Zusammenarbeit, Garantieregelungen, Bürgschaftssicherheiten oder Nutznießungen. Wiederum, keiner weiß besser Bescheid über die Möglichkeiten, als die Parteien selber.

Der Grundstein von Mediation ist der gemeinschaftliche Wunsch, zu einem Vergleich zu kommen. Keiner soll verlieren; alle sollen, auf welche Art und Weise auch immer, gewinnen. Mediation zielt darauf ab, den Konfliktfall zu lösen und den weiteren Projektverlauf durch eine positive Zusammenarbeit der Partner zu sichern. Wichtig für den Erfolg ist der Einsatz eines neutralen Dritten, der, ohne Entscheidungen zu treffen, die Partner in ihrer Suche nach Übereinstimmung lenkt.

Vorteile der Mediation

Wichtige Vorteile der Mediation sind geringe Kosten, gesparte Zeit, fortgesetzte Kontrolle und unbeschädigtes Image. Die Kosten sind normalerweise erheblich niedriger als bei Gerichtsverfahren und Arbitrage. Mediation konzentriert sich auf Materie und Lösung – also Inhalt statt Form –, es wird weniger oder kein Bedürfnis da sein, Juristen und Rechtsanwälte einzuschalten. Der Zeitaufwand ist niedriger, da beide Parteien die Notwendigkeit, zu einem Vergleich zu kommen, einsehen und keine Rücksicht gegenüber Behörden zu üben brauchen. Da die Parteien immer selber am Lenkrad bleiben, behalten für sie auch die Kontrolle. Die Lösung wird auf den Wünschen beider Parteien basieren und nicht auf einem Gesetz oder einer Vorschrift, die mit dem eigentlichen Problem nichts zu tun haben. Der letzte Vorteil ist die Beschränkung des Imageschadens. Parteien, welche nicht öffentlich Müll abladen, werden auch nicht zur Schau gestellt.

Mediationsablauf

Der Prozeß der Mediation läuft folgendermaßen ab:

- Die Parteien einigen sich auf einen Mediator. Wichtig ist, daß ein Vertrauensverhältnis zwischen den auftraggebenden Parteien und dem Konfliktlösungsspezialist vorhanden ist bzw. schnell aufgebaut wird.
- Der Mediator startet das Mediationsverfahren, indem er einen Kodex aufstellt, der beschreibt, welche Rechte und Pflichten den Beteiligten zukommen. Da Mediation ein freiwilliger Versuch ist und keine Garantie für die angestrebte Konfliktlösung gewährt, ist es wichtig, die Rechte und Pflichten sowie die Vertraulichkeit festzulegen. Wenn die Vertraulichkeit nicht gewährleistet ist, könnte Offenheit während der Mediationsgespräche der einen oder andern (eventuell sogar beiden) Partei Schaden zufügen.
- Gemeinschaftlich erfolgt die Definition der vorliegenden Situation und das zu erreichende Ziel. Sodann gilt es festzulegen, welcher Pfad zu beschreiten ist, um dieses Ziel zu erreichen. Die Beschreibung der Situation hält den Projektstatus fest und erlaubt eine Analyse. Die Stärken und Schwächen der jeweiligen Position werden identifiziert. Das zukünftige Ziel wird durch ein gemeinsames Verständnis für das angestrebte Ergebnis bestimmt. Gleiches geschieht für die vorgesehene Vorgehensweise.
- Erst dann startet die tatsächliche Konfliktlösung. Die Konfliktlösung versucht, eine konstruktive Zusammenarbeit der Beteiligten unter wirtschaftlichen Aspekten (wieder)herzustellen. Dazu berücksichtigt sie auf kreative Weise alle Möglichkeiten,

bis eine akzeptable und akzeptierte Problemlösung erreicht wird.

■ Letztendlich werden die angestrebten Ergebnisse protokolliert und bekommen einen rechtlich gültigen Status als Neuvertrag oder Vertragserweiterung. Essentielle Teile sind die Beschreibung der Vorgehensweise, die gegenseitigen Verantwortlichkeiten und die Zustimmung beider Seiten zum Vertrag.

■ Die eigentlichen Mediationsarbeiten sind damit beendet. Die Praxis dahingegen lehrt, dass die Parteien es bevorzugen, während des weiteren Projektablaufes den Konfliktlösungsspezialisten beizubehalten bzw. einzubeziehen, um die Emotionen in den Projekten zu managen und neue oder wieder auftretende Probleme rechtzeitig zu erkennen und zu lösen.

Erfolgsgrad

Mediation hat sich über die letzten Jahre in der Praxis als eine effektive Vorgehensweise zur Lösung wirtschaftlicher Konflikte und Probleme bewährt. Der Erfolgsgrad der Mediation ist hoch: In 70 bis 80 Prozent der Fälle wird eine Übereinstimmung erreicht. Dieser Erfolgsgrad wird gerade in den Bereichen erreicht, wo man ein hohes Maß an Spezialisierung antrifft: Bereiche wie IT-Management, Risikomanagement und Informationssicherheit.

Der ideale Mediator

Der Mediator soll der neutrale Dritte sein, der als Mittler Objektivität beisteuert und bei der Problemlösung hilft. Das stellt hohe Ansprüche an

die soziale Kompetenz des Mediators. Nicht nur Einfühlungsfähigkeiten und Verhandlungsvermögen spielen eine Rolle, sondern auch Faktoren wie Seniorität und Charisma sind hier äußerst wichtig.

Soziale Kompetenz alleine ist jedoch noch nicht genug, um bei Problemen mit Projekten, Software, Hardware und Dienstleistungen in den Bereichen IT-Management, Risikomanagement und Informationssicherheit Hilfe zu stellen. Der Mittler muß auch materieverbundene Qualifikationen haben:

- Fachmann mit nachgewiesener Erfahrung in den angesprochenen Problembereichen
- Unabhängig, unvoreingenommen und glaubwürdig für beide Seiten
- Erfahrung, Konflikte zu lösen im allgemeinen und Mediation im speziellen
- Projektführungserfahrung, um die Mediationsergebnisse so zu gestalten, daß die Zukunft des Projektes klar, möglich und praktikabel ist
- Erfahrung mit Vertragsausarbeitung, damit das Mediationsergebnis als Beweismittel zur Verfügung steht, wenn die Parteien sich (leider) dennoch entschließen, ein Zivilverfahren zu initialisieren.

Heute gibt es mehrere Berufsvereine für Mediatoren, wo erfahrene Sachverständige und Juristen sich zusammengetan haben. Die Berufsvereine bieten auch Arbitragedienstleistungen nach ihren eigenen Verfahrensweisen, die normalerweise allerdings sehr formell beschrieben sind. Die sorgfältige Protokollierung der Abwicklung erhöht den Status der Resultate und ermöglicht die weitere Benutzung der Resultate durch den

Richter, wenn die Parteien die Ergebnisse eines Schiedsgerichtes bzw. Schlichtungsverfahrens nicht akzeptieren.

Derzeit bieten noch wenige Beratungsgesellschaften und EDV-Revisoren Mediatordienste als festen Teil ihrer Dienstleistungspalette an. Eine Ursache könnte sein, dass ein Mediator, zusätzlich zu seinen Fähigkeiten auch noch einen guten Ruf sowie einen gewissen Bekanntheitsgrad haben muss. Solche Personen sind rar. Ein anderer Grund wird sicherlich sein, dass Mediation als Lösungsinstrument im EDV-Bereich noch ziemlich unbekannt ist, sicherlich weniger bekannt als das Prozessieren und das Aufgeben. Oder vielleicht ist es noch einfacher: Unter Umständen haben wir uns schon so an Projekte gewöhnt, die ihr Ziel nicht erreichen, länger dauern oder mehr kosten, so dass diese Situation an sich keinen Konflikt mehr auslöst...

Roeland Stouthart, Wien

Zum Autor

Roeland Stouthart hat sich als Berater für IT-Management größerer Unternehmen spezialisiert. Er hat fünf Jahre für KPMG im Information Risk Management in den Niederlanden gearbeitet und implementiert zur Zeit den Prozess der Informationssicherheit bei einer UN-Organisation in Wien.

The ISACA Crossword Puzzle 2/03

Dieses Rätsel ist auf deutsch und hat mit dem Schwerpunktthema dieser Nummer zu tun. Autor ist der Redaktor. Lösungen, Kommentare und Reklamationen sind an ihn zu richten.

Waagrecht: 1 tagfertig (schweiz); 5 hinterster Mast; **9 gesichtslos**; 14 Brühe; 15 Wasserguss (mundart); 17 Kanton der Schweiz; 18 Weltorganisation; 19 Trans World; 20 Lurch; 21 Zeichen (Mz); 23 Joanne Woodward hatte als solche drei Gesichter; 25 Fluss zur Elbe; 27 recht südlicher Richtmast (Abk); 29 Metallleiter; 31 Bahnhof (frz); 33 Schnee (ital); 34 entweder fehlt ein „e“ oder es ist am falschen Platz für diesen französischen Vornamen; 35 Tierhand; 37 Comic-Lacher; 38 wenn in die Hosen, dann ein Hasenfuss; 41 kopfloses Getreide; 42 AZ aus der Innerschweiz; 43 Schweizer Rheinzufluss; 44 pers Fürwort; 46 Vorname der Schauspielerin Palmer; 48 moderne Übermittlungsform im Geschäftsleben (Abk); **49 Zugangshilfe**; 54 die ersten drei Buchstaben eines unserer Länder; 56 nordische Totengöttin; **57 so darf 49 waagrecht eben nicht sein**; 58 electronic laser code (Abk); 59 aromatisches Getränk; 61 spanischer Artikel; 62 schnell; 64 kurzer Augenblick; 65 Stier; 67 Unterwürfigkeit; 70 Bein (engl); 71 Gattin von Menelaos, wenn sie Italienerin gewesen wäre; 73 mit „e“ angehängt, der Trank des Vergessens; 74 des Iren Heimat; 75 Geck; 76 österreichischer Alpenpass im Genitiv; 78 Hochplateau; 80 Ger-

1	2	3	4	5	6	7	8	9	10	11	12	13
14			15	16				17			18	
19		20					21			22		
	23	24			25	26		27				28
29			30			31	32		33			
		34			35	36			37			
38	39				40			41				42
43						44	45		46		47	
48			49	50	51		52		53		54	55
56			57								58	
		59	60			61			62	63		
64			65			66	67	68	69			
		70			71	72			73			
74				75				76				77
		78		79		80	81			82		
	83				84		85	86	87		88	89
90			91			92					93	
94					95				96			

mane; 82 Esel (frz); 83 Gedichtform (Mz); **85 Rassenbezeichnung**; 88 AZ aus der Westschweiz; 90 geladenes Atom; 91 Zeitbegriff; 92 Salatpflanze; 93 Fluss in Schottland; 94 kreuzen; 95 schlechtes Benehmen; 96 Drehkörper.

Senkrecht: 1 starker Zweig; 2 Edelstein; 3 geheimnisvolle Ausstrahlung; 4 selbstlautloser Schnellfahrer; 5 Tessiner Berg; 6 Muse; 7 kleine Brücke; 8 Anfang und Ende des Alphabets; 9 Baum (frz); 10 nordischer Männername; **11 manchmal reduziert sich alles darauf**; 12 Yield North-East (Abk); 13 erster Werktag (Abk); 16 durchlässig; 17 Konjunktion; 20 Gegenteil von alle; 21 noch eine Muse; 22 Verdioper; 24 genesen; 26 des Lateiners eigene Person; **28 unkenntlich Gemachtes**;

29 existierendes; 30 Zeichnerutensilien; **32 Tabelle**; 36 Gemütszustand; 37 Farbe des Lindenblattes; **39 Verschlüsselungsform**; 40 Glocke (Mz); 45 das Unsterbliche (Mz); **47 vernichten**; 50 AZ von Calw; 51 häufiger Name in China; 52 seine (span); 53 Fortpflanzungszelle; 55 Nordlandtier; 60 Fläche (Mz); 63 verwandt; 66 Nachruf; 68 Liebhaber (österreich); 69 Arbeitswille; 70 Zitrusfrucht; 72 ehemaliger Bestimmungsort (Abk); 75 Teufel; **77 Gesetz**; 79 Stadt in Südfrankreich; 81 Verpackungsgewicht; 83 ehemalige franz Münze; 84 AZ aus der Ostschweiz; 86 Bestand; 87 Metall; 89 drei gleiche Buchstaben; 90 Intelligenzquotient; 92 AZ von Konstanz; 93 kurze Dienstleistung.

Die Lösung liegt in den markierten Feldern. Dieses Wort ist auf einer Postkarte zu senden an M.F. Bretscher, Oberrenggstrasse 8, CH-8135 Langnau a/A bis 10. Juni 2003. Lösungen werden auch entgegen- genommen unter der Adresse mbretscher@kpmg.com.

Solution Crossword Puzzle 01/03:

Overreaction

The winner is Marc Bucher.
Congratulations!

Across: 1 revelation; 10 reap; 13 aside; 14 bullpen; 16 Ito; 18 IHR; 19 sen; 20 Po; 21 let; 23 Vetter; 25 orb; 26 Rhea; 27 abacus; 29 SE; 30 il; 31 TSC; 33 entrado; 34 ave; 35 at; 36 to; 37 dam; 38 menthol; 42 statics; 45 confidentiality; 48 prudent; 49 horrid; 51 res; 53 TI; 54 ee; 55 ode; 56 eternal; 60 YNM; 62 Di; 63 UN; 64 beacon; 65 gala; 66 Ute; 67 Celtic; 69 OSI (ISO); 70 CS; 71 Fes; 72 ego; 73 os; 74 Noa (-Noa); 76 passing; 78 least; 80 salt; 81 disclosure.

Down: 1 railroad; 2 est; 3 violet; 4 Ed; 5 lest; 6 TR; 7 object; 8 nurture; 9 else; 10 REN; 11 en; 12 problems; 15 personal- ity; 18 Ivanhoe; 20 privacy; 22 eastern; 24 TSA; 28 BE; 32 conferences; 34 adit; 38 mouse; 39 tin; 40 HDT; 41 LNH; 42 Sir; 43 tar; 44 tidings; 45 credits; 47 tobacco; 48 products; 60 separate; 52 pretend; 57 EBL; 58 NAIGGI; 59 lo; 61 Mainau; 68 Esso; 69 Oslo; 71 fat; 75 OSR; 76 PL, 77EC; 79 es.

There were several mistakes in this crossword puzzle, most of them un- intentional. One Watson found that horizontal words cannot stand on their head. And the auto plate CS no longer exists. A bad one was that 22 down and 48 across do not match. Most disciples of Watson found the missing number 46, but that was not what the author had intended. Sorry,

he pays US\$ 50 into the jackpot as a fine. The hidden mystery was sup- posed to be that it is not (as all others are) symmetric; the blank in 34 down and 49 across is not in the symmetry! And that mystery was not detected. Jackpot to be won next time US\$ 150! Keep looking for the oddities, Watson.

News aus den Interessengruppen

Neue Interessengruppen

Wir planen, neue Interessengruppen zu gründen. Als mögliche Themen sind vorgeschlagen:

- IG Continuous Auditing
- IG e-security (z.B. Attack and Penetration, e-defense, e-security Architecture)
- IG Archivierung (Aktualisierung der Arbeiten der ehemaligen IG Aufbewahrung)
- IG ??? Anregungen für weitere IGs nimmt Rolf Merz gerne entgegen.

IG Einführung von IT Governance

Leitung a.i.:
Rolf Merz
Ernst & Young AG
Brunnhofweg 37
Postfach 5032
3001 Bern
Tel. +41 58 286 66 79
Fax. +41 58 286 68 27
rolf.merz@eycom.ch

Die ehemalige IG Anwendung von COBIT wird mit einer angepassten Zielsetzung reaktiviert.

Kick-off-Sitzung: Freitag, 9. Mai 2003, 09.00–12.00 Uhr, bei Ernst & Young AG, Bleicherweg 21, 8022 Zürich

Urs Fischer hält ein Einführungs- referat zur Einführung von IT Govern- ance und stellt die neuesten Ent- wicklungen von ISACA/ISACF vor. Anschliessend Bildung der IG.

Anmeldung bis 2. Mai 2003 an Rolf Merz.

IG e-business

Leitung a.i.:
Rolf Merz
Ernst & Young AG
Brunnhofweg 37
Postfach 5032
3001 Bern
Tel. +41 58 286 66 79
Fax. +41 58 286 68 27
rolf.merz@eycom.ch

IG Outsourcing/ Insourcing

Ueli Engler
KPMG Fides Peat
Badenerstrasse 172
8004 Zürich
Tel. +41 1 249 26 16
uengler@kpmg.com

Nächste Sitzung: Offen. Interessenten melden sich bei Ueli Engler.

Mögliche Themen:

- Kontinuität des Insourcers
- Abhängigkeit vom Insourcer (Konkurs)
- Überarbeitetes Rundschreiben EBK
- Fernwartung, etc.

Geplant sind Herbstgespräche zum Thema „Grounding“ eines IT Service Providers mit ausgewählten Gesprächspartnern aus den Bereichen Legal, Service Provider, Industrie und Financial Services.

IG MIS/EIS/DWH

Leitung:
Daniel Oser
Ernst & Young AG
Badenerstrasse 47
Postfach 5272
8022 Zürich
Tel. +41 58 286 34 39
Fax. +41 58 286 32 76
daniel.oser@eycom.ch

Letzte Sitzung: Die letzte Sitzung fand am 25. März 2003 bei Ernst & Young am Bleicherweg in Zürich statt.

Folgende Themen wurden besprochen:

■ Referenzmodell Data Load: Das Referenzmodell beinhaltet sowohl den Top-Down als auch den Bottom-Up-Ansatz beim Erstellen eines Data Warehouses. In der letzten Sitzung wurde eine Erweiterung für die Schritte des Extrahierens und Ladens der Flat Tables diskutiert. Da bei den meisten Projekten Tools im Einsatz sind, welche mehrere Schritte des Referenzmodells abdecken, scheint es sinnvoll, diese Tools im Referenzmodell als Variante ebenfalls zu berücksichtigen.

■ Risk Matrix: Die Risk Matrix wurde in insgesamt drei halbtägigen Workshops unter den Revisoren der IG MIS dem Referenzmodell angepasst und vervollständigt. In dieser Sitzung wurde sie nun dem Plenum präsentiert. Die Consultants der IG werden nun die Risk Matrix plausibilisieren und allenfalls Vorschläge machen.

■ Project Management: In einem Brainstorming-Workshop anlässlich der nächsten Sitzung sollen DWH-spezifische Aspekte des Project Managements identifiziert und aufgelistet werden. Das Ziel ist eine Checkliste „Was muss im Minimum berücksichtigt werden“.

■ Reporting: Die Aspekte der Informationsverwendung aus einem DWH oder MIS sind bis anhin ausgeklammert worden. In einer zweiten Phase widmet sich die IG – nach Beendigung der ersten Themen – diesem Topic.

Nächste Sitzung: Noch offen. Voraussichtlich in der Kalenderwoche 19. Für Informationen wenden Sie sich bitte an Daniel Oser. Weitere

Mitglieder sind stets herzlich willkommen!

IG SAP R/3

Monika E. Galli Mead
Eidg. Finanzkontrolle
Monbijourstrasse 51a
3003 Bern
Tel. +41 31 324 9495
Fax. +41 31 323 1101
monika.galli@efk.admin.ch

Letzte Sitzung: Donnerstag, 14. November 2002, bei PWC, Zürich

Traktanden:

- ACL/Berechtigungen wie prüfen (Hr. Appl., SNB)
- Qualitätsprüfungskonzept im SAP (Hr. B. Bolli, CCSAP BAIT)
- Im SAP das Risk Assessment Tool RAT einsetzen (Hr. A. Hilsbos, PWC)
- Neues vom Jahresmeeting SAP-AK's (H.J. Stritter, EDV-Audit-Consult)
- Übertragung von SAP Walldorf (M. Galli)
- SAP und AIS AUDITool News, Erfahrungen und Tips (alle)

Nächste Sitzung: Termin noch offen. Interessenten melden Sie bitte bei der IG-Leiterin.

IG Romandie

Vacant : tous personnes intéressées à participer ou animer un groupe de travail ou tous ceux qui aimeraient proposer un thème de réflexion peuvent s'annoncer auprès de M. Paul Wang.
paul.wang@ch.pwcglobal.com

Express Line

A Word from the Chair

Each year, the Membership Board recognizes the vital role that chapters play in ensuring membership satisfaction and growth. Since 1989, the K. Wayne Snipes Award honors chapters that meet/exceed special service goals and recognizes active support in local membership.

We are proud to announce the 2002 winners of the K. Wayne Snipes Award:

- Asia: Medium chapter: Pune, Large chapter: Hong Kong
- Central/South America: Small chapter: Venezuela, Medium chapter: Costa Rica
- Europe/Africa: Medium chapter: Slovenia, Large chapter: Milan
- North America: Small chapter: Hawaii, Medium chapter: Hudson Valley (New York), Large chapter: National Capital Area (Washington, DC)
- Oceania: Medium chapter: Wellington
- Best Worldwide: Small chapter: Hawaii, Medium chapter: Wellington, Large chapter: National Capital Area

The Membership Board commends these chapters for all of their hard work and dedication to the success of ISACA(r).

Howard Nicholson
Chair, Membership Board

Certification Update

Maintaining CISA Status

Please remind members to remit annual maintenance fees and report continuing professional education hours for 2002 if they have not already done so. Failure to comply can result in CISA revocation.

2003 CISA and CISM Review Courses

The CISA and CISM review courses (detailed PowerPoint presentations) are available for chapter download at www.isaca.org/@chapter/cisa_edu/index.htm#cisa and www.isaca.org/@chapter/cism_edu/index.htm#cism.

These courses are designed to assist chapters as they help members and local candidates prepare for the CISA and CISM exams. Each course closely follows the material in the respective review manual.

CISM Study Material

The CISM Review Manual is available in the ISACA Bookstore. The manual features detailed descriptions and explanations of task and knowledge statements and it provides references to applicable information security management principles, practices and strategies.

CISM Applicant Update

A steady number of experienced information security managers continue to apply for CISM certification under the grandfathering provision. Some statistics relative to those who have applied thus far include:

- 84 percent have 10 years or more of information security experience
- 84 percent work in organizations with more than 100 employees
- 81 percent have been previously certified
- 79 percent have more than four years of university education
- 51 percent are CISA certified
- 39 percent are CISSP certified

The application period for CISM certification under the grandfathering provision ends on 31 December 2003.

Individuals without the required experience are encouraged to sit for the CISM exam on 14 June 2003, which will be held at the same time and locations as the CISA exam. Please encourage members and other industry professionals to visit the ISACA web site to download the appropriate forms at www.isaca.org/cism.htm.

DACH-News

D: Aktivitäten des German Chapter

Die herausragenden Ereignisse der letzten Monate waren einerseits wie jedes Jahr zu dieser Zeit die Mitgliederversammlung des ISACA German Chapter am 6. März im Frankfurter Hilton Hotel und andererseits die erstmalige Teilnahme des ISACA German Chapter als Aussteller auf der diesjährigen CeBIT in Hannover (s. Artikel in dieser Ausgabe des *NewsLetters*).

Fast 40 Mitglieder haben die Mitgliederversammlung in diesem Jahr besucht. Am Vormittag startete die Veranstaltung zuerst mit einem Vortrag von Herrn Hans-Georg Büttner zum Thema „Wireless Security“. Nach der Beantwortung und Diskussion von Fragen zum gehörten Vortrag, setzten sich die Gespräche beim folgenden Mittagessen im Hotel fort.

Auf der am frühen Nachmittag beginnenden Jahresmitgliederversammlung wurden die Vereinsaktivitäten des letzten Jahres sowie die angedachten Vorhaben durch den Vorstand präsentiert. Der bisherige Vorstand wurde für das abgelaufene Jahr entlastet. Bevor die Wahl eines neuen Vorstands begann, wurde eine Satzungsänderung zur Abstimmung gestellt und beschlossen. Hiernach werden ab sofort die Mitglieder des Vorstands für zwei und nicht mehr wie zuvor für ein Jahr gewählt. Aus dem bisherigen Vorstand schied das Vorstandsmitglied Georgios Safaridis auf eigenen Wunsch aus. Nach

der Aufnahme etwaiger Anwärter für die vorhandenen Vorstandsposten wurden die verbleibenden Vorstandsmitglieder in offener Wahl erneut bestätigt. Für den Vorstandsposten Konferenzen wurde Herr Markus Gaulke in den Vorstand gewählt und nimmt somit den Platz von Herrn Safaridis ein. Der neue Vorstand für die kommenden zwei Jahre ist auf den Seiten des German Chapter unter www.isaca.de wiederzufinden. Abgerundet wurde die Mitgliederversammlung mit einem Vortrag zum Berufsexamen des Certified Information Security Managers (CISM) durch Ingo Struckmeyer, die Initiierung der ersten Workgroup zum Thema Linux, der Herr Neuy vorsteht, sowie die Vorstellung einer Arbeitsgruppe der Gesellschaft für Informatik (GI) zum Thema Sicherheit, Schutz und Zuverlässigkeit durch Herrn Behnsen. Das Protokoll der Mitgliederversammlung wird demnächst noch separat an alle Mitglieder versandt.

An dieser Stelle möchten wir natürlich auch unserem ausgeschiedenen Vereinsvorstand Herrn Georgios Safaridis (bisher: Vorstand Konferenzen) ganz herzlich danken. Herr Safaridis hat sich nicht nur in den letzten vier Jahren direkt im Vorstand engagiert sondern auch viele Impulse regional im Hamburger Raum gesetzt. Hierzu zählte als herausragendes Ereignis die Arbeitsgruppe zum Thema COBIT mit dem abschließenden Pilotworkshop über zwei Tage in Hamburg, den er maßgeblich mitorganisierte. Wir hoffen

natürlich alle, dass er uns weiterhin als aktives Mitglied im ISACA German Chapter erhalten bleibt und wünschen ihm weiterhin alles Gute.

Die Mitgliederentwicklung mit mehr als 500 Mitgliedern sowie die Kassensituation des Vereins sind sehr erfreulich. Dies ermöglicht dem German Chapter auch die Unterstützung aktiver regionaler Arbeitsgruppen sowie der neu vorgestellten Workgroups. Weitere Informationen zu Arbeitsgruppen oder Workgroups sowie die Unterstützung durch das German Chapter finden sich in unserem Mitgliederbereich unter www.isaca.de oder lassen sich über Herrn Wojtyna erfragen.

Die diesjährigen CISA Vorbereitungskurse des German Chapters werden in Hamburg und Frankfurt ab dem 26. April stattfinden. Die im letzten Jahr überarbeitete Struktur in der Form von Wochenendseminaren an jeweils zwei Wochenenden und einem abschließenden CISA Testexamen als Generalprobe in Frankfurt wird beibehalten. Weitere Informationen auch für Nachzügler sind unter www.isaca.de zu finden.

Zum Schluss möchten wir noch alle Mitglieder dazu auffordern, den *NewsLetter* verstärkt als Basis für den Wissens- und Erfahrungsaustausch zu nutzen sowie die Möglichkeit in den neuen Workgroups mitzuarbeiten oder auch eine Workgroup ins Leben zu rufen zu nutzen, da der Berufsverband letztlich von den Aktivitäten seiner Mitglieder lebt.

Ingo Struckmeyer

Brief der Präsidentin

Liebe Mitglieder des ISACA German Chapter,

Am 7. März hat die Mitgliederversammlung mich wieder zur Präsidentin des Vereins gewählt. Für das Vertrauen bedanke ich mich sehr herzlich. Meine Vereinsvorstände Norbert Gröning, Heinrich Geis, Ingo Struckmeyer, Bernd Wojtyna und Michael Schneider stehen für Kontinuität und unser neues Vorstandsmitglied Markus Gaulke steht für neue Ideen.

Georgios Safaridis, der aus privaten Gründen aus dem Vorstand ausgeschieden ist, danke ich ganz herzlich für die gute Unterstützung in den letzten Jahren.

Karin Thelemann
Präsidentin

ISACA German Chapter e.V. auf der CeBIT 2003

In diesem Jahr präsentierte sich der Berufsverband der EDV-Revisoren (ISACA German Chapter e.V.) erstmalig in der Zeit vom 12. bis zum 19. März 2003 dem Fachpublikum auf der CeBIT in Hannover.

Der Messestand des ISACA German Chapter befand sich in Halle 17 Stand C 31/8 im Rahmen der Sonderschau CeFIS (Centrum für Informationssicherheit). Dieses Messeeareal wurde von der von zur Mühlen'schen Unternehmensberatung GmbH (VZM) organisiert und

beherbergte unter einem Dach unterschiedliche Unternehmen, die auf dem Gebiet der IT-Sicherheit tätig sind. Der Schwerpunkt der Aussteller in der Halle 17 war das Thema IT-Sicherheit. Zu diesem Thema waren neben dem ISACA German Chapter auch weitere nicht-kommerzielle Anbieter wie z.B. das Bundesamt für Sicherheit in der Informationstechnologie (BSI) vertreten.

Im CeFIS-Ausstellerforum präsentierte sich der Berufsverband täglich interessierten Zuhörern mit Kurzreferaten hauptsächlich zur Tätigkeit des Berufsverbandes selbst sowie zu den Themen IT-Governance, COBIT und weiteren Sachgebieten, auf denen der Berufsverband international Grundlagenarbeit leistet.

Während der achttägigen Messe wurde der Stand von den Mitgliedern des Vorstandes des ISACA German Chapter und von engagierten Mitgliedern des Berufsverbandes betreut, denen wir auf diesem Wege noch einmal unseren Dank für die

professionelle Unterstützung aussprechen möchten.

Im Laufe der Messe informierten sich mehr als 70 Fachbesucher konkret über die Produkte und Leistungen des internationalen Berufsverbandes und die Arbeit des ISACA German Chapters. Besonderes Interesse dabei fanden die Themen:

- CISA (Certified Information Systems Auditor)
- CISM (Certified Information Security Manager)
- COBIT (Control Objectives for IT)

Neben dem Berufsexamen CISA, das in erster Linie für Fachkräfte aus dem externen und internen Prüfungswesen interessant ist, galt die besondere Aufmerksamkeit der Besucher der neu angebotenen Zusatzqualifikation des Certified Information Security Managers.

Die Interessenten für das diesjährige CISA-Examen erkundigten sich vor allem über das Angebot zu den Vorbereitungskursen zur CISA-Prüfung,



Vortrag durch Karin Thelemann

die dieses Jahr wieder in Frankfurt und Hamburg stattfinden werden. Das Berufsexamen zum CISM fand hauptsächlich aus karrierebedingten Gründen das Interesse der Standbesucher. Auch Einsteiger in die freie Wirtschaft wie z.B. Berufssoldaten erkundigten sich, ob das Ablegen des CISM-Examens die beruflichen Möglichkeiten für das zukünftige Berufsleben verbessern könnte. Mitarbeiter von Unternehmensberatungen aus dem IT-Security-Umfeld versprechen sich über die CISM-Qualifikation bessere Wettbewerbschancen. Weitere Interessenten zum CISM-Examen befanden sich offensichtlich in der Situation sich beruflich neu orientieren zu müssen, wobei das Berufsexamen als Sprungbrett in eine weitere Berufslaufbahn dienen sollte. Besucher, die Auskunft zu COBIT

Besucher aus dem Ausland (Russland, Türkei, Baltische Länder) erkundigten sich hauptsächlich nach Kontaktmöglichkeiten zu den lokalen Chaptern in diesen Ländern.

Somit war festzustellen, dass das Interesse am ISACA auch international beim Fachpublikum der CeBIT vorhanden war. Zwischen den Vertretern des ISACA German Chapter und den Besuchern ergaben sich somit viele interessante Gespräche, die sicherlich die geleistete Arbeit wieder aufwogen.

Heinrich Geis

CH:

**Voranzeige: EUROCACs 2004
in der Schweiz**

Entgegen unserer Erwartungen und entsprechenden Kommunikation an der letzten Generalversammlung wurde Zürich als Ort der Durchführung für die EUROCACs 2004 gewählt. Das freut uns natürlich riesig! Aufgrund unserer Erfahrungen aus der Konferenz 1999 wissen wir, dass es einiges zu organisieren und abzuklären gibt. Freiwillige Helferinnen und Helfer sind deshalb gesucht! Meldungen nimmt vorläufig die Redaktion entgegen. Derzeit prüfen wir übrigens Alternativen für den Durchführungsort. Datum der Konferenz: 21.–24. März 2004.



ISACA Stand mit Michael Schneider und Michael Isensee

suchten, waren hauptsächlich daran interessiert, wie COBIT im praktischen Einsatz als Grundlage für die Ausgestaltung einer IT-Infrastruktur und zu deren Prüfung eingesetzt werden könnte.

Veranstaltungen

PKI – Public Key Infrastructure	6./7. Mai 2003 Karlsruhe, 2 Tage, Secorvo
PKI für Fortgeschrittene	8. Mai 2003 Secorvo, 1 Tag, Karlsruhe
CISA Testprüfung 2003	10. Mai 2003 Zürich, 1 Tag, ISACA
Informationstechnologie für Wirtschaftsprüfer und Finanzrevisoren	12.–15. Mai 2003 Zürich, 4 Tage, ISACA
IT Audit School	12.–16. Mai 2003 London, 5 Tage, MIS
Securing and Auditing Windows 2000 Server	13.–16. Mai 2003 London, 4 Tage, MIS
Lotus Notes Security	10.–21. Mai 2003 Secorvo, Karlsruhe
IT Audit & Control	11.–13. Juni 2003 London, 3 Tage, MIS
Neuigkeiten in der Überwachung von Zahlungs- und Effektenabwicklungssystemen	18. Juni 2003 Bern, 1 Tag, ISACA/Kammerseminar
e-biz Security Lab	8.–10. Juli 2003 Rapperswil, 3 Tage, ISACA
SAP R/3 für Wirtschafts- und Informatikprüfer	12.–15. August 2003 Stuttgart, 4 Tage, ISACA
Internet Security Lab	20.–22. August 2003 Zürich, 3 Tage, ISACA
Application Security Lab	27.–29. August 2003 Zürich, 3 Tage ISACA

Kontaktadressen Veranstalter

Der *NewsLetter* empfiehlt folgende Veranstalter (weitere Kurse und Unterlagen direkt anfordern):

AFAI
 Tel. +33 1 55 62 12 22
 afai@afai.asso.fr
 www.afai.asso.fr

advanced technology seminars
 Grundgasse 13
 CH-9500 Wil
 Tel. +41 71 911 99 15
 Fax. +41 71 911 99 16
 Maurer@inf.ethz.ch

Datenschutzbeauftragter des Kantons
 Zürich
 IT-Sicherheitsberatung und
 -Revision
 Andrea Carlo Mazzocco, CISA
 Kurvenstrasse 31
 CH-8090 Zürich
 Tel. +49 1 259 46 08
 Fax. +49 1 259 51 38
 andreacarlo.mazzocco@dsb.zh.ch
 www.datenschutz.ch

e-tec Security
 PO Box 54
 Wilmslow Chesire SK9 6FU
 United Kingdom
 info@a-tecsecurity.com

Euroforum Deutschland GmbH
 Hans-Günther-Sohl-Strasse 7
 D-40235 Düsseldorf
 Tel. +49 211 96 86 300
 Fax. +49 211 96 86 509
 info@euroforum.com

Hochschule für Technik Rapperswil
 Institut für Internet Technologien
 und Anwendungen
 Oberseestrasse 10
 8640 Rapperswil
 Tel. +41 55 222 41 11
 Fax. +41 55 222 44 00
 office@hsr.ch

IIR-Akademie
 Ohmstr. 59
 D-60468 Frankfurt/Main
 Tel. +49 69 7137 69-0
 Fax. +49 69 7137 69-69
 iir.academie@iir-ev.de

Integralis GmbH
 Gutenbergstr. 1
 D-85737 Ismaning
 Tel. +49 89 94573 447
 Fax +49 89 94573 199 fx
 schulung@integralis.de

ISACA CH
 Kurssekretariat
 c/o. Bitterli Consulting AG
 Konradstr. 1
 8005 Zürich
 Tel. +41 1 440 33 60
 Fax. +41 1 440 33 61
 kurse@isaca.ch

ISACA USA
 3701 Algonquin Rd #1010
 USA_Rolling Meadows IL 60008
 Tel. +1 847 253 15 45
 Fax. +1 847 253 14 43
 www.isaca.org

Marcus Evans
 Weteringschans 109
 1017 SB, Amsterdam
 The Netherlands
 Tel. +31 20 531 28 13
 Fax. +31 20 428 96 24
 www.marcusevansnl.com

MIS Training Institute
 Nestor House
 Playhouse Yard P.O. Box 21
 GB-London EC4V 5EX
 Tel. +44 171 779 8944
 Fax. +44 171 779 8293
 www.misti.com

MediaSec AG
 Tägerstrasse 1
 8127 Forch/Zürich
 Tel. +41 1 360 70 70
 Fax. +41 1 360 77 77
 it@mediasec.ch

Secorvo Security Consulting GmbH
 Secorvo College
 Albert-Nestler-Strasse 9
 D-76131 Karlsruhe
 Tel. +49 721 6105-500
 Fax +49 721 6105-455
 info@secorvo.de
 www.secorvo.de

Treuhand-Kammer
 Jungholzstrasse 43
 Postfach
 CH-8050 Zürich
 Tel. +41 1 305 38 60
 Fax. + 41 1 305 38 61

ZfU Zentrum für
 Unternehmensführung AG
 Im Park 4
 CH-8800 Thalwil
 Tel. +41 1 720 88 88
 Fax. +41 720 08 88
 info@zfu.c

Germany Chapter

Vereinsadressen

Geschäftsstelle

ISACA e.V., German Chapter
Eichenstr. 7
D-46535 Dinslaken
Tel. +49 2064 733191
Fax. +49 2064 733192
isaca.dinslaken@t-online.de

Präsidentin

Karin Thelemann
Ernst & Young AG
Wirtschaftsprüfungsgesellschaft
Mergenthalerallee 10–12
65760 Eschborn/Frankfurt am Main
Tel. +49 6196 99626 488
Fax. +49 6196 99626 449
karin.thelemann@de.ey.com

Konferenzen

Markus Gaulke

Mitgliederverwaltung und

Kassenwart

Norbert Gröning
PwC Deutsche Revision AG
Friedrich-List-Str. 20
D-45128 Essen
Tel. +49 201 438 0
Fax. +49 201 438 1000
Norbert.Groening@
de.pwcglobal.com

Public Relations

Heinrich Geis
Deutsche Börse AG
Neue Börsenstrasse 1
D-60487 Frankfurt
Tel. +49 692 101 5149
Fax. +49 692 101 4396
heinrich.geis@deutsche-boerse.com

Arbeitskreise und Facharbeit

Bernd Wojtyna
WLSGV-Prüfungsstelle
Regina-Portmann-Strasse 1
D-48159 Münster/Westfalen
Tel. +49 251 288 4253 oder
+49 251 210 4539
bernd_wojtyna@gmx.net

Publikationen

Ingo Struckmeyer
comdirect bank AG
Internal Audit
Pascalkehe 15
25451 Quickborn
Tel. +49 4106 704 1233
Fax. +49 4106 704 1990
ingo.struckmeyer@comdirect.de

CISA-Koordinator

Michael M. Schneider
Deloitte & Touche
Schumannstraße 27
60325 Frankfurt am Main
Tel. +49-69 75606 121
Fax. +49-69 75695 84448
michaelschneider@deloitte.de

Austria Chapter

Vereinsadressen

Vorsitzender (Präsident)

Ing. Mag. Dr. Michael Schirmbrand,
CIA, WP, StB
Europa Treuhand Ernst & Young
Praterstraße 23
1020 Wien
Tel: +43 1 211 70-2831
michael.schirmbrand@at.eyi.com

Stellvertretender Vorsitzender I (Vizepräsident I)

Dipl.-Ing. Maria-Theresia Stadler,
Österreichische Kontrollbank
Aktiengesellschaft
Strauchgasse 1–3
1010 Wien
Tel: +43 1 531 27-857
maria-theresia.stadler@oekb.co.at

Stellvertretender Vorsitzender II (Vizepräsident II)

Mag. Josef Renner, StB
GRT Price Waterhouse
Prinz-Eugen-Straße 72
1040 Wien
Tel: +43 1 50188-0

Sekretär

Mag. Gunther Reimoser, CISA
Europa Treuhand Ernst & Young
Praterstraße 23
1020 Wien
Tel: +43 1 21170-4113
gunther.reimoser@at.eyi.com

Kassier

Mag. Helmut Zödl
IBM Österreich
Obere Donaustraße 95
1020 Wien
Tel: +43 1 21145-0
helmut_zödl@at.ibm.com

CISA-Koordinator

Mag. Maria Rieder
Münze Österreich AG
Am Heumarkt 1
1010 Wien
Tel: +43 1 71715-0
maria.rieder@aon.at

Public Relations/Newsletter- Koordination

Rolf von Rössing
MA, D.E.s.s, CBCP, MBCI
Europa Treuhand Ernst & Young
Praterstraße 23
1020 Wien
Tel: +43 1 211 70-2812
dk@cos-ag.de

E-Mail ISACA Austria Chapter:

office@isaca.at

Homepage ISACA Austria Chapter:

www.isaca.at

Switzerland Chapter

Vereinsadressen

Präsidentin

Daniela S. Gschwend
Swiss Re
Mythenquai 50/60
8022 Zürich
Tel. +41 43 285 69 36
Fax. +41 43 285 33 69
daniela_gschwend@swissre.com

Vizepräsident

Michel Huissoud, CISA, CIA
Eidg. Finanzkontrolle/
Contrôle fédéral des finances
Monbijoustr. 45
3003 Bern
Tel. +41 31 323 10 35
Fax. +41 31 323 11 00
Michel.Huissoud@efk.admin.ch

Kassier

Pierre A. Ecoeur, CISA
Thurgauer Kantonalbank
Bankstr. 1
8570 Weinfelden
Tel. +41 71 626 64 61
Fax. +41 71 626 63 60
p.ecoeur@tkb.ch

Ausbildung/Kurssekretariat

Peter R. Bitterli, CISA
Bitterli Consulting AG
Konradstr. 1
8005 Zürich
Tel. +41 1 440 33 60
Fax. +41 1 440 33 61
prb@bitterli-consulting.ch

CISA/CISM-Koordinator

Thomas Bucher
Ernst & Young AG
Postfach
8022 Zürich
Tel. +41 58 286 42 90
Fax. +41 58 286 40 14
thomas.bucher@eycom.ch

Sekretär

c/o Präsidentin

Information & Kommunikation

Monika Josi
PricewaterhouseCoopers
Nordstr. 15
8035 Zürich
Tel. +41 1 630 27 82
Fax. +41 1 630 27 55
monika.josi@ch.pwcglobal.com
Adressmutationen bitte hier melden.

Koordinator Interessengruppen

Rolf Merz
Ernst & Young AG
Brunnhofweg 37
Postfach 5032
3001 Bern
Tel. +41 58 286 66 79
Fax. +41 58 286 68 27
Rolf.Merz@eycom.ch

Représentant Suisse Romande

Paul Wang
PricewaterhouseCoopers
Avenue Giuseppe Motta 50
1211 Genève 2
Tel. +41 22 748 56 01
Fax. +41 22 748 53 54
paul.wang@ch.pwcglobal.com

Marketing

Rigistrasse 3
CH-8703 Erlenbach
Tel. +41 1 910 96 33
Handy: +41 79 776 09 82
bru.wiederkehr@bluewin.ch

Homepage ISACA Switzerland
Chapter: www.isaca.ch